International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

# A Comprehensive Review On Expedite Message Authentication Protocol

**Divya Boya[1], Sravya Boya[2]**
[1]*Assistant Professor, Arjun College of Technology and Science*
[2]*Assistant Professor, Arjun College of Technology and Science*

**Abstract:**In vehicular networks, moving vehicles are enabled to communicate with each other through inter vehiclecommunications as good as with road-side units (RSUs) in neighborhood through roadside-to-vehicle communications. To be certain nontoxic operation of VANETs and increase the quantity of reliable information won from the bought messages, every OBU will have to be equipped to determinethe revocation popularity of all the received certificates in a timely method.Most of the current works lost sight of the authentication lengthen due to checking the CRL for each and every bought certificates. It introduce an expedite message authentication protocol (EMAP) which replaces the CRL checking approach by using an efficient revocation checking method making use of a fast and cozy HMAC perform and novel key sharing scheme using probabilistic random key distribution which enables an OBU to replace its compromised keys despite the fact that it earlier neglected some revocation messages.

**Keywords-**Vehicular networks, communication security, message authentication, certificate revocation.

## I. INTRODUCTION

An Ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the useof existing network infrastructure or centralized administration. Vehicular Ad-hoc Networks (VANETs) is a form of ad-hocnetwork which provides communication among the nearby vehicles. Vehicular ad hoc networks (VANETs) have attractedextensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadbandcommunication services to vehicles.

The VANETs architecture consists of a backbone network including authorities and management centers, equipmentinstalled beside the roads, namely Road Side Units and the corresponding devices inside the vehicles, namely the On-BoardUnits.

**Existing system**

• In VANETs, the primary security requirements are identified as entityauthentication, message integrity, non-repudiation, and privacy preservation.

• A well-recognized solution to secure VANETs is to deploy Public KeyInfrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managingthe revoked certificates.

• In PKI, each entity in the network holds an authentic certificate, and every messageshould be digitally signed before its transmission.

**Demerits**

1) Variety of attacks such as injecting false information
2) Modifying and replaying the disseminated messages can be easily launched.
3) A security attack on legitimate users.
4) The scale of VANET is very large.

## II. RELATED WORK

**Eviction of Misbehaving and Faulty Nodes in Vehicular Networks inthe year of 2007 by M.**

**Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P.Hubaux.**

- Misbehaving or faulty network node to be detected and removed
- Revocation using Compressed Certificate Revocation Lists (RC2RL) is used
- LEAVE protocol is used
- Event data recorders (EDRs), embeded in vehicle

**Merits**

1) security is a critical factor and a significant challenge to be met.
2) eviction is efficiently feasible and achieves a sufficient level of robustness.

**Demerits**

- There is a slight decrease in performance at very high densities
- The average speed is much higher, and performance decreases slightly for veryhigh speeds'
- Only consider for revocation
- Delay will be occure

**TACKing Together Efficient Authentication, Revocation, and Privacyin VANETs-2009 By A. Studer, E. Shi, F. Bai, and A. Perrig,**

- It consisting of a central trusted authority and regional authorities (RAs) distributedall over the network.
- The trusted authority acts as the group manager and the vehicles act as thegroup members.

**Merits**

- Efficiently prevents eavesdroppers from linking a vehicle's different keys
- Identify the valid vehicle
- Less overhead for vehicle to vehicle communication

**Disadvantage**

- TACK not suitable for the safety applications in VANETs as the WAVEstandard,
- This certificate is valid only within the coverage range of the RA.

**K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security CertificateRevocationList Distribution for VANET," Proc. Fifth ACM int'lWorkshop VehiculAr InterNETworking, pp. 88-89, 2008.**

• In a VANET, a certificate authority issues keys and certificates to vehicles.
• Each vehicle distributes these certificates to other VANET participants
• Every vehicle must sign the certificate for security purpose.

**Merits**

• Epidemic distribution of certificate revocation lists which is quick andefficientEfficiently distribute the certificate
• Certificate authority check the certificate status Car-to-car epidemic distribution of certificate revocation lists

**Demerits**

• Only employ the road side unit Distribution point
• Certificate Revocation List is consisting large certificate
• Their is no Timestamp

**An Efficient Pseudonymous Authentication Scheme withStrong Privacy Preservation for Vehicular Communications in the yearof 2010 by Yipin Sun, Student Member, IEEE, Rongxing Lu, StudentMember, IEEE, Xiaodong Lin, Member, IEEE**

•PASS supports Roadside Unit aided distributed certificate service
•PASS allows the vehicles to update certificates on road,
• It provide privacy for certificate

**Merits**

• Optimize revocation overhead
• Reducing certificate overhead

**Demerits**

• Can not trace legitimate vehicle
• Can't provide location privacy

**Pseudonym Changing at Social Spots: An EffectiveStrategy for Location Privacy in VANETs in the year of 2012 by RongxingLu,**

**Member, IEEE, Xiaodong Lin, Member, IEEE, Tom H. Luan,XiaohuiLiang, Student Member, IEEE, and Xue min (Sherman) Shen, Fellow, IEEE**

• As a prime target of Quality of Privacy (QoP) in ks (VANETs),
• If the pseudonyms are changed in an improper time and location, such solution is
invalid

**Advantage**

• It present an effective pseudonym changing at social spot
Provable location privacy

**Demerits**

• It is not possible to track the vehicle exactly

Haas et al. [6] develop a mechanism to reduce the size of the broadcast CRL by only sending a secret key perrevoked vehicle. On receiving the CRL, each OBU uses the secret key of each revoked vehicle to construct the completeCRL. It should be noted that although the broadcast CRL size is reduced, the constructed CRL at each OBU, which isused to check the revocation status of other entities, still suffers from the expected large size exactly as that in thetraditional CRLs where all the identities of the certificates of every revoked OBU are included in the broadcast CRL.

A different way of reducing the size of the CRL involves using types of compression techniques. One method forcompressing the CRL information using Bloom filters was introduced by in [14] . In this method, each certificate that is revokedis hashed to a fixed number of bits several times. The resulting hash value for each revoked certificate forms a type of signature.The signatures of several revoked certificates can be combined into a single bit sequence that serves as the Bloom filter. Eachtime a certificate is received, the same hashes are performed and the resulting value is checked against the Bloom filter. If thesignature matches a pattern in the Bloom filter, that means the certificate has been revoked with high probability. Storing CRLinformation in this manner compresses the size of the CRL considerably since a fixed-length Bloom filter is distributed insteadof distributing 8 to 14 bytes for every certificate that is revoked.There is a small probability of a false positive occurring when using this method due to hash collisions, which increasesas more certificates are added to the Bloom filter. [15] suggests testing a new pseudonym against the currently-possessed Bloomfilter to see if the new pseudonym tests positive (revoked) using the Bloom filter. If the pseudonym does test positive, the usershould discard the pseudonym and try a different one.In [17] a mechanism is introduced to reduce the size of the broadcast CRL by only sending a secret key per revoked vehicle. Onreceiving the new CRL, each OBU uses the secret key of each revoked vehicle to reproduce the identities of the certificates

## III. PROPOSED WORK

Expedite Message authentication protocol (EMAP) which replaces theCRL checking process by an efficient revocation checking processusing a fast and secure HMAC function. EMAP is suitable not only forVANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce theauthentication delay resulting from checking the CRL in VANETs.EMAP has the lowest computation complexity compared with the CRL checkingprocesses employing linear and binary search algorithms.The number of messages that can be verified using EMAP within 300 msec isgreater than that using linear and binary CRL checking by 88.7 and 48.38percent, respectively. The proposed EMAP in authentication reduces the end-to-end delay compared withthat using either the linear or the binary CRL checking process.

**Development of VANET architecture:**

The Vehicular Adhoc Network model consists of Trusted Authority (TA), RoadsideUnits (RSUs), On-Board Units (OBUs). Trusted Authority, which is responsible for providing certificates and distributing secret keys to all OBUs in the network. Roadside Units which are fixed Units distributed all over the network. On-Board Units, which are embedded in

vehicles. OBUs can communicate eitherwith other OBUs through V2V communications or with RSUs through V2Icommunications.

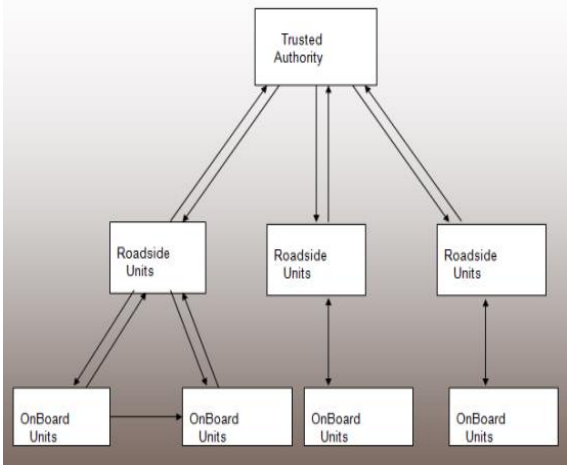


Fig.1 Overview of the system

**Message Authentication:**

If an OBU want to communicate other OBU means it send an encrypted messagewith a HMAC code using HMAC algorithm, it generate by using the sender id andcommon secret key which knows all the unrevoked OBUs.The receiver OBU also generates the HMAC code by using common secret key. Whether the HMAC code is same means the receiver knows the sender OBU is anauthenticated OBU otherwise not process the message

## IV. CONCLUSION

Aoriginal key sharing mechanism allows an OBU toupdate its compromised keys even if it previously missed some revocation message s. Also EMAP has a modular featurerendering it integral with any PKI system. Moreover, it is resistant to common attacks while outperforming the authenticationtechniques employing the conventional CRL. This means that EMAP can appreciably decrease the message loss ratio due tomessage verification delay compared to the conventional authentication methods employing CRL checking.

## REFERENCES

[1] Albert Wasef and Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for VehicularAd Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.1 YEAR 2013.

[2] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicularcommunication systems: a position paper," Proc. Workshop on Standards for Privacy in User-Centric IdentityManagement, Zurich, Switzerland, July 2006. 29

[3] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providinglocation privacy for VANET," Proc. Embedded Security in Cars (ESCAR), November 2005.

[4] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicularnetworks," IEEE Trans. on Vehicular Technology, vol. 59, pp. 533–549, 2010.

[5] M. Raya and J.-P.Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1,pp. 39–68, 2007.

[6] "US bureau of transit statistics." [Online]. Available: http://en.wikipedia.org/wiki/Passenger vehicles in theUnited States.

[7] J. J. Haas, Y. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanismfor VANET," Proc. 6th ACM international workshop on VehiculArInterNETworking, pp. 89–98, 2009.

[8] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications andmanagement messages," IEEE Std 1609.2-2006, 2006.

[9] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

[10] "FCC Report and Order 99-305," 1999.

[11].P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular CommunicationSystems," Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.

[12].A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy inVANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9, 2009.

[13].M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in VehicularNetworks," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[14]. J.J. Haas, Y. Hu, and K.P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism forVANET," Proc.Sixth ACM International Workshop Vehicular Inter NETworking, pp. 89-98, 2009.

[15]. S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-HocNetworks,"2006.

Authors:

Divya Boya Completed M.Tech (SE) and working as Asst. Professor in Arjun College of Technology and Science.

Sravya Boya Completed M.Tech (SE) and working as Asst. Professor in Arjun College of Technology and Science.